Cyclic Codes Over a Nonchain Ring

Shakila Banu. P.[1] and Suganthi .T.[2]
[1]Assistant Professor, Department of Mathematics, Vellalar College for Women, Thindal,
Erode-638012, Tamil Nadu, India.
[2]B.T.Assistant of Mathematics, Govt. Higher Secondary School, Vadugam,Namakkal-637408, Tamil Nadu, India.

Abstract

In this paper, a non-chain ring $\mathrm{R} = \mathbb{Z}_3 + w\mathbb{Z}_3 + w^2\mathbb{Z}_3 + w^3\mathbb{Z}_3, w^4 = w$. The ring acquires its ideals and maximal aspirations. Cyclic Codes over R were characterised in terms of their structure and generators. Additionally, the parameters of several quantum error-correcting codes are found using the cyclic and negacyclic codes over R. Many different systems for information storage and retrieval can be built using these codes.

Keywords: Cyclic Codes, Idempotent generators, Negacyclic Codes, and Quantum codes.
2020 MSC : 94B15,94B60,81P70.

I. Introduction

Coding theory originated in the late 1940s and had its roots in engineering. It is the branch of communication theory that deals with the mathematical study of codes with a view to their employment in communication systems, usually for the purpose of increasing their efficiency and reliability. The algebraic structure of linear codes is suitable for both encoding and decoding. Since the 1960s, linear codes over finite rings have been used. The most significant linear code in coding theory is the cyclic code. E. Prange [16] was the first to study cyclic codes. Cyclic codes are widely studied because of their algebraic structure and good error correction capability. The structure of cyclic, quasi-cyclic, and cons acyclic codes is defined over finite rings [3, 20]. A lot of work has been done on cyclic code over finite rings. Simeon Ball [17] described the various kinds of cyclic codes and how to use them to create designs. There is a generator for each cyclic code.

Chen et al.'s [6] method of factoring the polynomial X_2 m pn-1 over a finite field led to the discovery of the generators of cyclic codes. The generators of cyclic codes with odd length and their dual codes over $\mathbb{Z}_4$ were addressed by Abualrub [1]. Cyclic codes of length 2 k were categorised in [10] over the Galois ring GR (4, m). B.R.MC. Donald [13] examined the elements in finite rings. Under the gray map from $\mathbb{Z}_4$ to $\mathrm{F}_2{}^2$, certain suitable nonlinear codes can be found as the binary images of various cyclic codes. Such works inspire me to conduct research on chain rings. They [11,19] examined the structure of cyclic codes and the quantity of codewords over finite chain rings $\mathbb{Z}_4 + \mathrm{u}\mathbb{Z}_4$ and $\mathbb{Z}_q + \mathrm{u}\mathbb{Z}_q$.

Mohammed [15] achieved the generalization of cyclic codes over $\mathrm{F}_q + \mathrm{uF}_q + \mathrm{u2}\ \mathrm{F}_q + \cdots + \mathrm{uk} - 1\ \mathrm{F}_q$ with arbitrary length. The structure of cyclic codes and their idempotents with odd length over F_q were obtained by Bocong Chen et al. [4]. Hai Q. Dinh [14] studied cyclic codes of p^s length over $\mathrm{F}_{p^m} + \mathrm{uF}_{p^m}$. Gao [11] investigated the cyclic codes over $\mathbb{Z}_q + w\mathbb{Z}_q$, where $w^2 = 0$ and q is the power of a prime. Several families of codes over finite rings were studied in [1,2,15] over $\mathbb{Z}_4, \mathbb{Z}_2 + \mathrm{v}\mathbb{Z}_2, \mathrm{v}^2 = \mathrm{v}; \mathbb{Z}_2 + w\mathbb{Z}_2 + \mathrm{v}\mathbb{Z}_2 + w\mathrm{v}\mathbb{Z}_2, w^2 = \mathrm{v}^2 = 0$; $\mathbb{Z}_p^r + w\mathbb{Z}_p^r + \cdots . + w^{k-1}\mathbb{Z}_p^r, w^k = 0$, where p is a prime.

According to the paper [12], self-dual cyclic codes of length n over F_q exist when both n and q are even. With the parameters $(\mathrm{n}, \mathrm{n} + 1/2)$ and $(\mathrm{n}, \mathrm{n} - 1/2)$, two binary cyclic codes were introduced, and they produced certain quadratic residue codes when n is prime. Previous research indicates that when $(\mathrm{n}, \mathrm{q}) = 1$, there is no cyclic self-dual code over F_q.

Constacyclic codes, which Wolfmann [18] first developed over a finite commutative ring, are a generalization of cyclic codes. In [8,9], they showed the repeated-root self-cyclic codes of length $3p^s$ over F_pm and generator polynomials of all constacyclic codes of length with multiples of 2,3, and 6 over $\mathrm{F}_pm + \mathrm{uF}_pm$ and calculated the number of codewords in each of those cyclic codes. Zhu [20], who looked at the constacyclic codes across non-chain rings, found that the constacyclic image underneath the gray map is linear cyclic.

M. Miwa [14] discussed even repeated root codes and length codes over a ring. He [3] obtained the generators of quasi-cyclic codes and the quantity of codewords. Many techniques and plenty of approaches are implemented to provide positive varieties of codes with precise parameters and properties. This examination of finite rings became precipitated after the accomplishment of gray maps. Calderbank [5] built quantum error-correcting codes from classical error-correcting codes. But Dertil [7] built many nice quantum codes with the help of cyclic codes over finite fields or finite rings with self-orthogonal (or dual containing) properties. In this paper, we define a non-chain ring $\mathrm{R} = \mathbb{Z}_3 + w\mathbb{Z}_3 + w^2\mathbb{Z}_3 + w^3\mathbb{Z}_3, w^4 = w$. The ideals and maximal ideals of the ring are acquired. The structure and generators of cyclic codes over R were determined. Moreover, from the cyclic and negacyclic codes over R , the parameters of some quantum errorcorrecting codes These codes have many applications in constructing information storage and retrieval systems.

This paper is structured as follows: Section II contains the fundamentals of coding theory. The Gray images of cyclic and quasi-cyclic codes over R are defined in Section III. A necessary condition for a code to be cyclic is given in Section IV. Finally, in Section V, some quantum error correction codes and their parameters are listed.

II. Preliminaries

In order to derive some cyclic codes over a ring, we must be aware of some fundamentals of coding theory. A subset I of a commutative ring $\mathfrak{R}$ is called an Ideal of $\mathfrak{R}$ if (i) I is a subring of R and (ii) I is closed under multiplication. An Ideal of a ring $\mathfrak{R}$ generated by one element is called principal ideal. If every ideal of $\mathfrak{R}$ is principal, then $\mathfrak{R}$ is a principal ideal ring. An ideal M of a ring $\mathfrak{R}$ is called a maximal ideal if $M \neq R$ and the only ideal containing M are M and $\mathfrak{R}$.Ideals M and N in a ring $\mathfrak{R}$ are called comaximal if $\mathrm{M} + \mathrm{N} = \mathfrak{R}$. Let $\mathfrak{R}$ be a ring. Then $\mathfrak{R}$ is called a chain ring if its ideals form a finite chain. A ring $\mathfrak{R}$ is called a local ring if the set of non-units of $\mathfrak{R}$ is closed under addition.

In coding theory, a linear code is an error-correcting code for which any linear combination of codewords is also a codeword. Linear codes are used in forwarding error correction and are applied in methods for transmitting symbols (e.g., bits) on a communications channel.

A linear code of length n and rank k is a linear subspace C with dimension k of the vector space F_{q^n} where F is the finite field. Such a code is called a QR code. The dual code $\mathrm{C}^{\perp}$ of C is $\mathrm{C}^{\perp} = \{x/\forall y \in \mathrm{C}, x.y = 0\}$ where $x = (x_0, x_1, \dots \dots, x_{n-1}), y = (y_0, y_1, \dots., y_{n-1})$. If $\mathrm{x}.\mathrm{y} = 0$, then x and y are said to be orthogonal. A code C is self-orthogonal if $\mathrm{C} \subseteq \mathrm{C}^{\perp}$.

A linear code C is cyclic if every cyclic shift of a codeword is a codeword. That is, $(\mathrm{c}_0, \mathrm{c}_1, \dots, \mathrm{c}_{n-1}) \in \mathrm{C}$ implies that $(\mathrm{c}_{n-1}, \mathrm{c}_0, \dots, \mathrm{c}_{n-2}) \in \mathrm{C}$. The dual of a cyclic code is also cyclic.

A constacyclic code is a linear code with the property that for some constant λ if $(\mathrm{c}_1, \mathrm{c}_2, \dots., \mathrm{c}_n)$ is a codeword, then so is $(\lambda\mathrm{c}_n, \mathrm{c}_1, \dots., \mathrm{c}_{n-1})$.A negacyclic code is a constacyclic code with $\lambda = -1$. The Hamming distance between two code words is the number of non-zero bits that are different between two-bit strings, and it is denoted by the function $\mathrm{d}(\mathrm{x}, \mathrm{y})$, where x and y are codewords. The Lee distance between two codewords $\mathrm{x}, \mathrm{y} \in Z_m^n$ is $\mathrm{d}_L(\mathrm{x}, \mathrm{y}) =$

$$\sum_{i=1}^{n} \min(|x_i - y_i|, m - |x_i - y_i|)$$

III. Gray map over $\mathbb{Z}_3 + \boldsymbol{w}\mathbb{Z}_3 + \boldsymbol{w}^2\mathbb{Z}_3 + \boldsymbol{w}^3\mathbb{Z}_3$

In this section, we study units, ideal structure, and the properties of the ring $\mathbb{Z}_3 + w\mathbb{Z}_3 + w^2\mathbb{Z}_3 + w^3\mathbb{Z}_3$. We introduce a Gray map.

Hereafter, $\mathrm{R} = \mathbb{Z}_3 + w\mathbb{Z}_3 + w^2\mathbb{Z}_3 + w^3\mathbb{Z}_3$, where $w^4 = w$ and $\mathbb{Z}_3 = \{0,1,2\}$ throughout this paper. It is a commutative ring with characteristic 3.Clearly $\mathrm{R} \cong \mathbb{Z}_3[w]/< w^4 - w >$.Any element $\mathring{\mathrm{r}}$ of R can be expressed uniquely as $\mathring{\mathrm{r}} = \mathrm{p} + \mathrm{q}w + \mathrm{r}w^2 + \mathrm{s}w^3$, where $\mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{s} \in \mathbb{Z}_3$.

For any $\mathring{r}_1, \mathring{r}_2 \in R$, the Lee distance is given by

$$\mathrm{d}_L\left(\mathring{\mathrm{r}}_1, \mathring{r}_2\right) = W_L\left(\mathring{\mathrm{r}}_1 - \mathrm{o}_2\right)$$

The maximal ideals of R with 27 elements.

$$\mathbf{1}. <w>=\{0,\ w,\ 2w,\ w^3,\ w+w^3,\ 2w+w^3, 2w^3, w+2w^3,\ 2w+2w^3, w^2, w+w^2,\\ 2w+w^2,\ w^2+w^3,\ w+w^2+w^3, 2w+w^2+w^3,\ w^2+2w^3,\\ w+w^2+2w^3, 2w+w^2+2w^3,\ 2w^2, w+2w^2, 2w+2w^2,\ 2w^2+w^3,\\ w+2w^2+w^3,\ 2w+2w^2+w^3,\ 2w^2+2w^3,\ w+2w^2+2w^3,\\ 2w+2w^2+2w^3\}$$

$$\mathbf{2}. <2+w>=\{0,\ 2+w,\ 1+2w,\ 2+w^3,\ 1+w+w^3,\ 2+w^3,\ 1+2w^3,\ w+2w^3,\\ 2+2w+2w^3,\ 2+2+2w^3,\ 2+w^2,\ 1+w+w^2,\ 2w+w^2,\ 1+w^2+w^3,\\ w+w^2+w^3,\ 2+2w+w^2+w^3,\ w^2+2w^3,\ 2+w+w^2+2w^3,\\ 1+2w+w^2+2w^3, 1+2w^2,\ w+2w^2, 2+2w+2w^2, 2w^2+w^3,\\ 2+w+2w^2+w^3, 1+2w+2w^2+w^3, 2+2w^2+2w^3, 1+w+2w^2+2w^3,\\ 2w+2w^2+2w^3\}$$

These two ideals $\langle w \rangle$ and $\langle 2+w \rangle$ are comaximal and R is a semi-local ring. That is $\langle w \rangle + \langle 2+w \rangle = \text{R}$.
The ideals with 81 elements that generate the ring R and also the generator of these ideals are the units of the ring.

$$<1>=<2>=<1+w>=<2+2w>=<1+w^3>=<2+w+w^3>=<1+2w+w^3>=<2+2w+w^3>\\ =<2+2w^3>=<1+w+2w^3>=<2+w+2w^3>=<1+2w+2w^3>=<1+w^2>=<2+w+w^2>\\ =<1+2w+w^2>=<2+2w+w^2>=<2+w^2+w^3>=<1+w+w^2+w^3>=<2+w+w^2+w^3>\\ =<1+2w+w^2+w^3>=<2+w^2+2w^3>=<1+w+w^2+2w^3>=<2+2w+w^2+2w^3>=<2+2w^2>\\ =<2+2w^2>=<1+w+2w^2>=<2+w+2w^2>=<1+2w+2w^2>=<1+2w^2+w^3>\\ =<1+w+2w^2+w^3>=<2+2w+2w^2+w^3>=<1+2w^2+2w^3>\\ =<2+w+2w^2+2w^3>=<1+2w+2w^2+2w^3>\ =<2+2w+2w^2+2w^3>$$

3. Zero ideal of R ,

$$< 0 >= \{0\}$$

since the ideals $\langle w \rangle$ and $\langle 2+w \rangle$ are not comparable, R is a non-chain ring.
Since $\mathbb{Z}_3$ is a field, then, its ideals are trivial ones. Since R does not have a unique maximal ideal, R is not the principal ideal ring.
The Gray map from $\mathbb{Z}_3 + w\mathbb{Z}_3 + w^2\mathbb{Z}_3 + w^3\mathbb{Z}_3$ to Z_3^4 is defined as follows:

$$\psi\text{: R} \rightarrow Z_3^4$$

$$(\text{p} + \text{q}w + \text{r}w^2 + \text{s}w^3) \rightarrow (\text{p}, \text{p} + \text{q} + \text{r} + \text{s}, \text{p} + 2\text{q} + \text{r} + 2\ \text{s}, \text{p} + \text{q} + 2\text{r} + 2\ \text{s})$$

For any $\mathring{r}_1 \in$ R, Lee weight of $\mathring{r}_1$ is $W_L\left(\mathring{r}_1\right) = W_H\left(\psi\left(\overset{r}{r_2}\right)\right)$.

The map ψ is an isometry that transforms the Lee distance. in the ring R to the Hamming distance in $\mathbb{Z}_3^4$.
The Gray map can be extended from R^n to $\mathbb{Z}_3^{4n}$.

Theorem: 3.1

The Gray map ψ is a distance preserving map from (R^n, Lee weight) to ($\mathbb{Z}_3{}^{4n}$, Hamming weight).Moreover it is an isometry from R^n to $\mathbb{Z}_3{}^{4n}$.

Proof:

For any $\mathring{r}_1, \mathring{r}_2 \in$ R and $\alpha \in \mathbb{Z}_3$.

$$\psi(\mathring{\mathrm{r}}_1+\mathring{\mathrm{r}}_2)=\psi(\mathring{\mathrm{r}}_1)+\psi(\mathring{\mathrm{r}}_2)$$
$$\psi(\alpha\mathring{\mathrm{r}}_1)=\alpha\,\psi(\mathring{\mathrm{r}}_1)$$

So ψ is linear.

$$\begin{aligned} d_L(\mathring{r}_1, \mathring{r}_2) = & W_L(\mathring{r}_1 - \mathring{r}_2) \\ & = W_H(\psi(\mathring{r}_1 - \mathring{r}_2)) \\ & = W_H(\psi(\mathring{r}_1) - \psi(\mathring{r}_2)) \\ & = d_H(\psi(\mathring{r}_1) - \psi(\mathring{r}_2)) \end{aligned}$$

ψ is a distance preserving map.

Theorem 3.2

If $\dot{r} = p + qw + rw^2 + sw^3$ of R is unit iff $p \neq 0$ and $p + q + r + s \neq 0(\mathrm{mod}3)$

Proof:

Let $\mathring{\mathrm{r}} = \mathrm{p}_1 + \mathrm{q}_1 w + \mathring{\mathrm{r}}_1 w^2 + \mathrm{s}_1 w^3$ is a unit of R .

Then $\mathring{r}_1 \cdot \mathring{r}_2 = 1(\mathrm{mod}3)$, where $\mathring{r}_2 = \mathrm{p}_2 + \mathrm{q}_2 w + \mathrm{r}_2 w^2 + \mathrm{s}_2 w^3$ is inverse of $\mathring{r}_1$.

$$(\mathrm{p}_1 + \mathrm{q}_1 w + \mathrm{r}_1 w^2 + \mathrm{s}_1 w^3)(\mathrm{p}_2 + \mathrm{q}_2 w + \mathrm{r}_2 w^2 + \mathrm{s}_2 w^3) = 1$$

since $\mathring{r}_1$ is unit, $\mathrm{p}_1 \cdot \mathrm{p}_2 = 1$.

Hence $\mathrm{p} \neq 0$.

Assume, $\mathrm{p}_1 + \mathrm{q}_1 + \mathring{\mathrm{r}}_1 + \mathrm{s}_1 \equiv 0(\mathrm{mod}3)$

Then $\mathrm{p}_1 = \mathrm{p}_2 = \mathrm{S}_2$

which is contradiction. Therefore $\mathrm{p} + \mathrm{q} + \mathrm{r} + \mathrm{s} \neq 0(\mathrm{mod}3)$.

If r is unit, then $\mathrm{p} \neq 0$ and $\mathrm{p} + \mathrm{q} + \mathrm{r} + \mathrm{s} \neq 0(\mathrm{mod}3)$. similarly,the converse part is also true.

Theorem:3.3

A ring R with unity is local, if the non-unit elements of R is an ideal of R.

Proof:

$\mathrm{R} - \mathrm{U(R)} = \{0, w^2, 2w^3, 2w, 1 + w + w^3 + \cdots.\}$, where $\mathrm{U(R)}$ = group of units of R .

since $R - U(R)$ does not satisfy associative property, R-U(R) is not an ideal of R.

Therefore, R is not a local ring.

Theorem: 3.4

If B is a linear code of length n over $\mathbb{Z}_3 + w\mathbb{Z}_3 + w^2\mathbb{Z}_3 + w^3\mathbb{Z}_3$ with
$|B| = 3$ and minimum Lee weight w_L then $\psi(B)$ is $[4n, k, d_H]$ ternary linear codes over $\mathbb{Z}_3$.

Theorem: 3.5

If B is self-orthogonal then ψ(B) is self orthogonal.

Proof:

Let B be self-orthogonal and
$\mathring{r}_1 = \mathrm{p}_1 + \mathrm{q}_1 w + \mathrm{r}_1 w^2 + \mathrm{s}_1 w^3, \overset{r}{r}_2 = \mathrm{p}_2 + \mathrm{q}_2 w + \mathrm{r}_2 w^2 + \mathrm{s}_2 w^3 \in \mathrm{B}$
Where $\mathrm{p}_1, \mathrm{p}_2, \mathrm{q}_1, \mathrm{q}_2, \mathrm{r}_1, \mathrm{r}_2, \ \mathrm{s}_1, \ \mathrm{s}_2 \in \mathbb{Z}_3$.

Since $\mathring{r}_1, \mathring{r}_2 = 0$,

$$(\mathrm{p}_1 + \mathrm{q}_1 w + \mathrm{r}_1 w^2 + \mathrm{s}_1 w^3) \cdot (\mathrm{p}_2 + \mathrm{q}_2 w + \mathrm{r}_2 w^2 + \mathrm{s}_2 w^3) = 0$$
$$\mathrm{p}_1\mathrm{p}_2 = \mathrm{p}_1\mathrm{q}_2 + \mathrm{p}_2\mathrm{q}_1 + \mathrm{s}_2\mathrm{q}_1 + \mathrm{r}_1\mathrm{r}_2 + \mathrm{q}_2\ \mathrm{s}_1 =$$
$$\mathrm{p}_2\mathrm{r}_1 + \mathrm{r}_1\ \mathrm{s}_2 + \mathrm{p}_1\mathrm{r}_2 + \mathrm{q}_1\mathrm{q}_2 + \mathrm{s}_1\mathrm{r}_2 = \mathrm{p}_1\ \mathrm{s}_2 + \mathrm{q}_1\mathrm{r}_2 + \mathrm{q}_2\mathrm{r}_1 + \mathrm{p}_2\ \mathrm{s}_1 = 0$$
$$\psi(\mathrm{r}_1) \cdot \psi(\mathrm{r}_2) = (\mathrm{p}_1, \mathrm{p}_1 + \mathrm{q}_1 + \mathrm{r}_1 + \mathrm{s}_1, \mathrm{p}_1 + 2\mathrm{q}_1 + \mathrm{r}_1 + 2\ \mathrm{s}_1, \mathrm{p}_1 + \mathrm{q}_1 + 2\mathrm{r}_1 + 2\ \mathrm{s}_1) \cdot (\mathrm{p}_2$$
$$\mathrm{p}_2 + \mathrm{q}_2 + \mathrm{r}_2 + \mathrm{s}_2, \mathrm{p}_2 + 2\mathrm{q}_2 + \mathrm{r}_2 + 2\ \mathrm{s}_2, \mathrm{p}_2 + \mathrm{q}_2 + 2\mathrm{r}_2 + 2\ \mathrm{s}_2)$$

Hence, ψ(B) is self orthogonal.

IV. Cyclic Codes over $\mathbb{Z}_3 + w\mathbb{Z}_3 + w^2\mathbb{Z}_3 + w^3\mathbb{Z}_3$

In this part, the structure of linear and cyclic codes over R is studied, and generators of cyclic (negacyclic) rings are generated.

Define

$$\mathrm{B}_1 = \{\mathrm{p} \in \mathbb{Z}_3 / \mathrm{p} + \mathrm{q}w + \mathrm{r}w^2 + \mathrm{s}w^3 \in \mathrm{B}\}$$
$$\mathrm{B}_2 = \{\mathrm{p} + \mathrm{q} + \mathrm{r} + \mathrm{s} / \mathrm{p} + \mathrm{q}w + \mathrm{r}w^2 + \mathrm{s}w^3 \in \mathrm{B}\}$$

$$\mathrm{B}_3 = \{\mathrm{p}+2\mathrm{q}+\mathrm{r}+2\ \mathrm{s}/\mathrm{p}+\mathrm{q}w+\mathrm{r}w^2+\mathrm{s}w^3 \in \mathrm{B}\}$$

$$\mathrm{B}_4 = \{\mathrm{p}+\mathrm{q}+2\mathrm{r}+2\ \mathrm{s}/\mathrm{p}+\mathrm{q}w+\mathrm{r}w^2+\mathrm{s}w^3 \in \mathrm{B}\}$$

Then B_1, B_2, B_3, and B_4 are ternary codes of length n . The linear code B of length n over R can be uniquely expressed as

$$\mathrm{B} = (1+2w+2w^2+w^3)\mathrm{B}_1 \oplus (2w+2w^2)\mathrm{B}_2 \oplus (2w^2+w^3)\mathrm{B}_3 \oplus (2w+w^3)\mathrm{B}_4$$

Theorem:4.1

Let B be a linear code of length n over R Then $\psi(B) = B_1 \otimes B_2 \otimes B_3 \otimes B_4$ and $|B| = |B_1||B_2||B_3||B_4|$

Proof:

For any $(\mathrm{p}_0, \mathrm{p}_1, \mathrm{p}_2, \dots . \mathrm{p}_{n-1}, \mathrm{p}_0+\mathrm{q}_0+\mathrm{r}_0+\mathrm{s}_0, \mathrm{p}_1+\mathrm{q}_1+\mathrm{r}_1+\mathrm{s}_1, \dots .$

$$\mathrm{p}_{n-1}+\mathrm{q}_{n-1}+\mathrm{r}_{n-1}+\mathrm{s}_{n-1}, \mathrm{p}_0+2\mathrm{q}_0+\mathrm{r}_0+2\ \mathrm{s}_0$$
$$\mathrm{p}_1+2\mathrm{q}_1+\mathrm{r}_1+2\ \mathrm{s}_1, \dots, \mathrm{p}_{n-1}+2\mathrm{q}_{n-1}+\mathrm{r}_{n-1}+2\ \mathrm{s}_{n-1}$$
$$\mathrm{p}_0+\mathrm{q}_0+2\mathrm{r}_0+2\ \mathrm{s}_0, \mathrm{p}_1+\mathrm{q}_1+2\mathrm{r}_1+2\ \mathrm{s}_1, \dots$$
$$\mathrm{p}_{n-1}+\mathrm{q}_{n-1}+2\mathrm{r}_{n-1}+2\ \mathrm{s}_{n-1}) \in \psi(\mathrm{B})$$

Let $\mathrm{m}_i = \mathrm{p}_i+\mathrm{q}_i w+\mathrm{r}_i w^2+\mathrm{s}_i w^3, \mathrm{i} = 0,1,2, \dots . \mathrm{n}-1.$

Since ψ is bijection

$$\mathrm{m} = (\mathrm{m}_0,\ \mathrm{m}_1, \dots . \mathrm{m}_{n-1}) \in \mathrm{B}$$

By the definition of B_1, B_2, B_3 and B_4,

we get,

$$(\mathrm{p}_0, \mathrm{p}_1, \mathrm{p}_2, \dots, \mathrm{p}_{n-1}) \in \mathrm{B}_1,$$
$$(\mathrm{p}_0+\mathrm{q}_0+\mathrm{r}_0+\mathrm{s}_0, \mathrm{p}_1+\mathrm{q}_1+\mathrm{r}_1+\mathrm{s}_1, \dots, \mathrm{p}_{n-1}+\mathrm{q}_{n-1}+\mathrm{r}_{n-1}+\mathrm{s}_{n-1}) \in \mathrm{B}_2,$$
$$(\mathrm{p}_0+2\mathrm{q}_0+\mathrm{r}_0+2\ \mathrm{s}_0, \mathrm{p}_1+2\mathrm{q}_1+\mathrm{r}_1+2\ \mathrm{s}_1, \dots, \mathrm{p}_{n-1}+2\mathrm{q}_{n-1}+\mathrm{r}_{n-1}+2\ \mathrm{s}_{n-1}) \in \mathrm{B}_3,$$
$$(\mathrm{p}_0+\mathrm{q}_0+2\mathrm{r}_0+2\ \mathrm{s}_0, \mathrm{p}_1+\mathrm{q}_1+2\mathrm{r}_1+2\ \mathrm{s}_1, \dots, \mathrm{p}_{n-1}+\mathrm{q}_{n-1}+2\mathrm{r}_{n-1}+2\ \mathrm{s}_{n-1}) \in \mathrm{B}_4$$

So,

$$\psi(\mathrm{B}) \subseteq \mathrm{B}_1 \otimes \mathrm{B}_2 \otimes \mathrm{B}_3 \otimes \mathrm{B}_4$$

For any $(\mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{s}) \in \mathrm{B}_1 \otimes \mathrm{B}_2 \otimes \mathrm{B}_3 \otimes \mathrm{B}_4$.

where,

$$\mathrm{p} = (\mathrm{p}_0, \mathrm{p}_1, \mathrm{p}_2, \dots, \mathrm{p}_{n-1}) \in \mathrm{B}_1$$
$$\mathrm{q} = (\mathrm{p}_0+\mathrm{q}_0+\mathrm{r}_0+\mathrm{s}_0, \mathrm{p}_1+\mathrm{q}_1+\mathrm{r}_1+\mathrm{s}_1, \dots, \mathrm{p}_{n-1}+\mathrm{q}_{n-1}+\mathrm{r}_{n-1}+\mathrm{s}_{n-1}) \in \mathrm{B}_2$$
$$\mathrm{r} = (\mathrm{p}_0+2\mathrm{q}_0+\mathrm{r}_0+2\ \mathrm{s}_0, \mathrm{p}_1+2\mathrm{q}_1+\mathrm{r}_1+2\ \mathrm{s}_1, \dots, \mathrm{p}_{n-1}+2\mathrm{q}_{n-1}+\mathrm{r}_{n-1}+2\ \mathrm{s}_{n-1}) \in \mathrm{B}_3$$
$$\mathrm{s} = (\mathrm{p}_0+\mathrm{q}_0+2\mathrm{r}_0+2\ \mathrm{s}_0, \mathrm{p}_1+\mathrm{q}_1+2\mathrm{r}_1+2\ \mathrm{s}_1, \dots, \mathrm{p}_{n-1}+\mathrm{q}_{n-1}+2\mathrm{r}_{n-1}+2\ \mathrm{s}_{n-1}) \in \mathrm{B}_4$$

Since B is linear,

$$\mathrm{m} = (1+2w+2w^2+w^3)x+(2w+2w^2)y+(2w^2+w^3)z+(2w+w^3)t \in \mathrm{B}$$
$$(\mathrm{m}) = (\mathrm{p}, \mathrm{q}, \mathrm{r}, \mathrm{s})$$
$$\mathrm{B}_1 \otimes \mathrm{B}_2 \otimes \mathrm{B}_3 \otimes \mathrm{B}_4 \subseteq \psi(\mathrm{B})$$
$$\text{Therefore, } \psi(\mathrm{B}) = \mathrm{B}_1 \otimes \mathrm{B}_2 \otimes \mathrm{B}_3 \otimes \mathrm{B}_4.$$
$$\psi(\mathrm{B}) = |\mathrm{B}_1 \otimes \mathrm{B}_2 \otimes \mathrm{B}_3 \otimes \mathrm{B}_4|$$
$$= |\mathrm{B}_1||\mathrm{B}_2||\mathrm{B}_3||\mathrm{B}_4|$$

Theorem: 4.2

For $i = 1,2,3,4$. If G_i 's are generator matrix of ternary linear codes B_i 's then the generator matrix of B is

$$\begin{pmatrix}(1+2w+2w^2+w^3)G_1\\(2w+2w^2)G_2\\(2w^2+w^3)G_3\\(2w+w^3)G_4\end{pmatrix}$$

Proof:

$$\psi(\mathrm{B})=\mathrm{B}_1\otimes\mathrm{B}_2\otimes\mathrm{B}_3\otimes\mathrm{B}_4=\begin{pmatrix}\psi(1+2w+2w^2+w^3)G_1\\\psi(2w+2w^2)G_2\\\psi(2w^2+w^3)G_3\\\psi(2w+w^3)G_4\end{pmatrix}$$

$$=\begin{pmatrix}G_1&0&0&0\\0&G_2&0&0\\0&0&G_3&0\\0&0&0&G_4\end{pmatrix}$$

Theorem:4.3

Let us consider $B=(1+2w+2w^2+w^3)B_1\oplus(2w+2w^2)B_2\oplus(2w^2+w^3)B_3\oplus(2w+w^3)B_4$ is a cyclic code over R iff B_i 's are cyclic codes for $i=1,2,3,4$.

Proof:

Let us consider $(\mathrm{p}_0,\mathrm{p}_1,\ldots.,\mathrm{p}_{n-1})\in\mathrm{B}_1,(\mathrm{q}_0,\mathrm{q}_1,\ldots.,\mathrm{q}_{n-1})\in\mathrm{B}_2,(\mathrm{r}_0,\mathrm{r}_1,\ldots.\mathrm{r}_{n-1})\in\mathrm{B}_3,(\mathrm{s}_0,\ \mathrm{s}_1,\ldots.,\mathrm{s}_{n-1})\in\mathrm{B}_4$.
Assume $\mathrm{m}_i=(1+2w+2w^2+w^3)\mathrm{p}_i+(2w+2w^2)+(2w^2+w^3)\mathrm{r}_i+(2w+w^3)\mathrm{s}_i$ for i $=1,2,\ldots.\mathrm{n}-1$.
Then $(\mathrm{m}_0,\ \mathrm{m}_1,\ldots.\mathrm{m}_{n-1})\in\mathrm{B}$. Since B is a cyclic code, $(\mathrm{m}_0,\ \mathrm{m}_1,\ldots.\mathrm{m}_{n-2})\in\mathrm{B}$.
Hence $(\mathrm{p}_{n-1},\mathrm{p}_1,\ldots.,\mathrm{p}_{n-2})\in\mathrm{B}_1,(\mathrm{q}_{n-1},\mathrm{q}_1,\ldots,\mathrm{q}_{n-2})\in\mathrm{B}_2,(\mathrm{r}_{n-1},\mathrm{r}_1,\ldots.\mathrm{r}_{n-2})\in\mathrm{B}_3,(\mathrm{s}_{n-1},\ \mathrm{s}_1,\ldots,\mathrm{s}_{n-2})\in\mathrm{B}_4$.
Therefore, $\mathrm{B}_1,\ \mathrm{B}_2,\ \mathrm{B}_3\ \ \mathrm{B}_4$ are cyclic codes over $\mathbb{Z}_3$.
Conversely,
Suppose that $\mathrm{B}_1,\ \mathrm{B}_2,\ \mathrm{B}_3$ and B_4 are cyclic codes over $\mathbb{Z}_3$. Let $(\mathrm{m}_0,\ \mathrm{m}_1,\ldots.\mathrm{m}_{n-1})\in\mathrm{B}$ where,
$\mathrm{m}_i=(1+2w+2w^2+w^3)\mathrm{p}_i+(2w+2w^2)+(2w^2+w^3)\mathrm{r}_i+(2w+w^3)\mathrm{s}_i$ for i $=1,2,\ldots.\mathrm{n}-1$.
Then $(\mathrm{p}_0,\mathrm{p}_1,\ldots,\mathrm{p}_{n-1})\in\mathrm{B}_1,(\mathrm{q}_0,\mathrm{q}_1,\ldots,\mathrm{q}_{n-1})\in\mathrm{B}_2,(\mathrm{r}_0,\mathrm{r}_1,\ldots.\mathrm{r}_{n-1})\in\mathrm{B}_3,(\mathrm{s}_0,\ \mathrm{s}_1,\ldots,\mathrm{s}_{n-1})\in\mathrm{B}_4$
Note that, $(\mathrm{m}_{n-1},\ \mathrm{m}_0,\ldots.\mathrm{m}_{n-2})=(1+2\mathrm{w}+2w^2+w^3)(\mathrm{p}_{n-1},\mathrm{p}_1,\ldots,\mathrm{p}_{n-2})$

$$\begin{gathered}+(2w+2w^2)(\mathrm{q}_{n-1},\mathrm{q}_1,\ldots,\mathrm{q}_{n-2})\\+(2w^2+w^3)(\mathrm{r}_{n-1},\mathrm{r}_1,\ldots.\mathrm{r}_{n-2})\\+(2w+w^3)(\mathrm{s}_{n-1},\ \mathrm{s}_1,\ldots.,\mathrm{s}_{n-2}))\in\mathrm{C}\end{gathered}$$

$=(1+2w+2w^2+w^3)\mathrm{B}_1\oplus(2w+2w^2)\mathrm{B}_2\oplus(2w^2+w^3)\mathrm{B}_3\oplus(2w+w^3)\mathrm{B}_4$
So, B is cyclic code over R.

Theorem: 4.4

Let $B=<(1+2w+2w^2+w^3)B_1\oplus(2w+2w^2)B_2\oplus(2w^2+w^3)B_3\oplus(2w+w^3)B_4$ be a cyclic(negacyclic) code of length n over R, Then $B=<(1+2w^2+w^3)f_1(x),(2w+2w^2)f_2(x),(2w^2+w^3)f_3(x),(2w+w^3)f_4(x)>$ and $|B|=3^{4n-(\Sigma\deg f_i(x))}$ where f_i 's are generator polynomials of B_i 's for i = 1,2,3,4.

Proof:

since B_i 's are cyclic codes over R ,
$\mathrm{B}=<(1+2w^2+w^3)f_1(x),(2w+2w^2)f_2(x),(2w^2+w^3)f_3(x),(2w+w^3)f_4(x)>$
By theorem 4.1, $|\mathrm{B}|=|\mathrm{B}_1||\mathrm{B}_2||\mathrm{B}_3||\mathrm{B}_4|$

$$\begin{gathered}=3^{n-\deg f_1}\,.\,3^{n-\deg f_2}\,.\,3^{n-\deg f_3}\,.\,3^{n-\deg f_4}\\=3^{4n-\sum_{i=1}^{4}\deg(f_i)}\end{gathered}$$

where f_1,f_2,f_3,f_4 are generator polynomials of B_1,B_2,B_3,B_4 respectively.

Corollary: 4.1

Let $B=<f(x)>$ be a negacyclic code of length n over R and $\psi(f(x))=(f_1,f_2,f_3,f_4)$ with $\deg\left(gcd(f_1,x^n+1)\right)=n-k_1,\deg\left(gcd(f_2,x^n+1)\right)=n-k_2,$

$\deg\left(gcd(f_3, x^n+1)\right) = n-k_3, \deg\left(gcd(f_4, x^n+1)\right) = n-k_4,$

Then $|B| = 3^{(k_1+k_2+k_3+k_4)}$.

Example: 4.1

Let B $=< f(x) >= (1+w^3)x^7 + wx^6 + (2+w^2)x^5 + w^2x^3 + x^2 + 2$ be a negacyclic code of length 13 over R .

$$\psi(f(x)) = (x^7+2x^5+2,2x^7+x^6+x^3+2,2x^6+x^3+2, x^6+x^5+2x^3+2)$$

$$f_1 = \text{gcd }(x^7+2x^5+2, x^{13}+1) = 1$$

$$f_2 = \text{gcd }(2x^7+x^6+x^3+2, x^{13}+1) = (x+1)(x^3+2x+1)$$

$$f_3 = \text{gcd }(2x^6+x^3+2, x^{13}+1) = (x+1)$$

$$f_4 = \text{gcd }(x^6+x^5+2x^3+2, x^{13}+1) = (x+1)$$

$$|B| = 3^{45}.$$

Let $\mathrm{h}_i(\mathrm{n}) = (x^n+1)/(\text{gcd }(f_i, x^n+1)$ $\mathrm{B}^\perp =< \psi^{-1}\left(\mathrm{h}_{1_R}(\mathrm{n}), \mathrm{h}_{2_R}(\mathrm{n}), \mathrm{h}_{3_R}(\mathrm{n}), \mathrm{h}_{4_R}(\mathrm{n})\right) >$ where h_{i_R} be the reciprocal polynomial of $\mathrm{h}_i(x)$ for i = 1,2,3,4.

$$\mathrm{B}^\perp =< \psi^{-1}(x^{13}+1, x^9+2x^8+2x^7+x^5+2x^3+x^2+1, x^{12}+2x^{11}$$
$$+x^{10}+2x^9+x^8+2x^7+x^6+2x^5+x^4+2x^3+x^2+2x+1$$
$$x^{12}+2x^{11}+x^{10}+2x^9+x^8+2x^7+x^6+2x^5+x^4$$
$$+2x^3+x^2+2x+1) >$$
$$=< (1+2w+2w^2+w^3)x^{13} + (2w+2w^2+2w^3)x^{12} + (w+w^2+w^3)x^{11} + (2w+2w^2+$$
$$2w^3)x^{10} + (w^3)x^9 + (2w^3)x^8 + (2w+2w^2+w^3)x^7 +$$
$$(2w+2w^2+2w^3)x^6 + (w^3)x^5 + (2w+2w^2+2w^3)x^4 +$$
$$(2w+2w^2+w^3)x^3 + (w+w^2+2w^3)x^2 + (w+w^2+w^3)x + 1) >$$

V. Quantum Codes from cyclic codes over R.

We examine the dual nature of cyclic and their generators in this section. Some cyclic (negacyclic) codes can be used to create quantum error-correcting codes.

Theorem:5.1

A cyclic code B with generator polynomial $f(x)$ contains its dual iff $x^n - 1 \equiv 0$ (mod $ff^*)f^*$ is reciprocal polynomial of f.

Proof:

The proof is trivial.

Theorem 5.2

Let $B =< (1+2w+2w^2+w^3)f_1, (2w+2w^2)f_2, (2w^2+w^3)f_3, (2w+w^3)f_4 >$ be a cyclic (negacyclic) code of length n over R. Then $B^\perp \subseteq B$ iff $x^n - 1 \equiv 0$ (modf $f_i, f_i^*)\left(x^n+1 \equiv 0(\mathrm{modf}_i, f_i{}^*)\right)$ for $i = 1,2,3,4$.

Proof:

Let $x^n - 1 \equiv 0(\mathrm{modf}_i, \mathrm{f}_i{}^*)\left(x^n+1 \equiv 0(\mathrm{modf}_i, \mathrm{f}_i{}^*)\right)$ for i = 1,2,3,4.

By using, $B_1^\perp \subseteq \mathrm{B}_1, B_2^\perp \subseteq \mathrm{B}_2, B_3^\perp \subseteq \mathrm{B}_3, B_4^\perp \subseteq \mathrm{B}_4,$

$$((1+2w+2w^2+w^3)B_1^\perp \oplus (2w+2w^2)B_2^\perp \oplus (2w^2+w^3)B_3^\perp \oplus (2w+w^3)B_4^\perp) \subseteq$$
$$((1+2w+2w^2+w^3)\mathrm{B}_1 \oplus (2w+2w^2)\mathrm{B}_2 \oplus (2w^2+w^3)\mathrm{B}_3 \oplus (2w+w^3)\mathrm{B}_4)$$

So,

$$< (1+2w+2w^2+w^3)f_1{}^*, (2w+2w^2)f_2{}^*, (2w^2+w^3)\mathrm{f}_3{}^*, (2w+w^3)f_4{}^*i > \subseteq$$
$$< (1+2w+2w^2+w^3)f_1, (2w+2w^2)f_2, (2w^2+w^3)f_3, (2w+w^3)f_4 >$$

That is, $\mathrm{B}^\perp \subseteq$ B.

Conversely,

suppose that $\mathrm{B}^\perp \subseteq$ B.

$$\left(1+2w+2w^2+w^{\overline{3}}\right)B_1^\perp \otimes (2w+2w^2)B_2^\perp \otimes (2w^2+w^3)B_3^\perp \otimes (2w+w^3)B_4^\perp \subseteq$$

$(1+2w+2w^2+w^3)\mathrm{B}_1 \otimes (2w+2w^2)\mathrm{B}_2 \otimes (2w^2+w^3)\mathrm{B}_3 \otimes (2w+w^3)\mathrm{B}_4$ under $\mathrm{mod}(1+2w+2w^2+w^3), \mathrm{mod}(2w+2w^2), \mathrm{mod}(2w^2+w^3)$ and $\mathrm{mod}(2w+w^3)$.

we have,

$$B_i^\perp \subseteq \mathrm{B}_i \text{ for i} = 1,2,3,4$$

Therefore,

$$x^n - 1 \equiv 0(\mathrm{mod} f_i, f_i{}^*) \text{ for i} = 1,2,3,4$$

Corollary: 5.1

$(1 + 2w + 2w^2 + w^3)B_1 \oplus (2w + 2w^2)B_2 \oplus (2w^2 + w^3)B_3 \oplus (2w + w^3)B_4$ is a cyclic (negacyclic) code of length n over R. Then $B^\perp \subseteq B$ iff $B_i^\perp \subseteq B_i$ for $i = 1,2,3,4$.

Theorem:5.3

$(1 + 2w + 2w^2 + w^3)B_1 \oplus (2w + 2w^2)B_2 \oplus (2w^2 + w^3)B_3 \oplus (2w + w^3)B_4$ is a cyclic (negacyclic) code of arbitrary length n over R with type $81^{k_1}27^{k_2}9^{k_1}3^{k_2}$. If $B_i{}^\perp \subseteq B_i$ where $i = 1,2,3,4$ then $B^\perp \subseteq B$ and there exists a quantum error-correcting code with parameter $[4n, (4k_1 + 3k_2 + 2k_3 + k_4) - 4n, d_L]$ where d_L is the minimum lee weights of B.

Example 5.1

Let $\mathrm{n} = 8$, we have $x^8 - 1$ in $\mathbb{Z}_3[\mathrm{x}]$.

Let $f_1(x) = f_2(x) = x^2 + 1, f_3(x) = f_4(x) = x^2 + 2x + 2$.

Thus $\mathrm{B} =< (1 + 2w + 2w^2 + w^3)f_1, (2w + 2w^2)f_2, (2w^2 + w^3)f_3, (2w + w^3)f_4 >$. B is a linear cyclic code of length 8.

Hence, we obtain a quantum code with parameters [32,12,2].

The parameters of Quantum codes

n	Generator Polynomials	[[N, K, D]]
8	$f_1(x) = f_2(x) = x^2 + 1, f_3(x) = f_4(x) = x^2 + 2x + 2$	[32,12,2]
12	$f_1(x) = f_2(x) = f_3(x) = f_4(x) = x + 2$	[48,38,2]
17	$f_1(x) = f_2(x) = f_3(x) = f_4(x) = x + 2$	68,58,2]
19	$f_1(x) = f_2(x) = f_3(x) = f_4(x) = x + 2$	76,66,2]
20	$f_1(x) = f_2(x) = x^2 + 1, f_3(x) = f_4(x) = x^5 + 2x^4 + 2x^3 + 2x^2 + 2x$	[80,51,2]
33	$f_1(x) = f_2(x) = f_3(x) = f_4(x) = x^5 + 2x^3 + x^2 + 2x + 2$	[132,82,2]
36	$f_1(x) = f_2(x) = x^2 + 1, f_3(x) = f_4(x) = x + 2$	[144,127,2]

References:

[1] TT.Abualrub and R.Oehmke,On the generators of Z4 cyclic codes of length2e,IEEE Transactions on InformationTheory,vol.49(9),pp.2126-2133,2003,DOI:10.1109/TIT.2003.815763 .

[2] T.Abualrub and I.Siap,Cyclic codes over the ring Z2+uZ2 andZ2+uZ2+u2 Z2 , Designs Codes and Cryptography,vol.42,pp.273-287,2007,DOI:10.1007/s10623-006-9034-5 .

[3] M.Bhaintwal, S.K.Wasan, On quasi-cyclic codes over Zq , Applicable Algebra in Engineering Communication and Computing, vol.20, pp.459-480,DOI:10.1007/s00200-009-0110-8,2009.

[4] Bocong Chen,Hongwei Liu,Guanghui Zhang,Some minimal Cyclic codes over nite _elds,Discrete Mathematics,vol.331,pp.142-150,DOI:10.1016/j.disc.2014.05.007,2014

[5] A.R.Calderbank,E.M.Rains,P.M.Shor,N.J.A.Sloane,Quantum error correctionvia codes over GF(4),IEEE Transactions on Information Thoery, vol.44,pp.1369-1387, 1998,DOI:10.1109/18.681315.

[6] Y. H. Chen, T. K. Truong, Y. Chang, C. D. Lee, and S. H. Chen, Algebraic decoding of quadratic residue codes using Berlekamp-Massey algorithm ,Journal of Information Science and Engineering, vol.23,pp.127-145,2007.

[7] A.Dertli,Y.Cengellenmis,S.Eren, On quantum codes obtained from cyclic codesover A2 ,International Journal of Quantum Information, Vol.13,no.3, pp.1550031,DOI:10.1142/S0219749915500318,2015.

[8] Hai.Q. Dinh, Constacyclic Codes of length ps over F pm+uF pm, Journal of Algebra,vol.324,no.5,pp.940-950,2010,DOI:10.1016/j.jalgebra.2010.05.027 .

[9] Hai.Q. Dinh, Structure of repeated-root constacyclic codes of length and their duals, Discrete Mathematics,vol.313,no.9,pp.983-991,2013,DOI:10.1016/j.disc.2013.01.024.

[10] S.T. Dougherty, S. Ling, Cyclic codes over Z4 of even length, Designs,Codes and Cryptography, vol.39,no.2,pp.127-153,2006,DOI:10.1007/s10623-005-2773-x.

[11] Gao,Jian and Fu,Fang-Wei and Xiao,Ling and Bandi, Ramakrishna,Some results on cyclic codes over Zq+uZq ,Discrete Mathematics, Algorithms and Applications,vol.07,no.4,2015,DOI:10.1142/S1793830915500585.

[12] Y. Jia, S. Ling and C. Xing, On Self-Dual Cyclic Codes Over Finite Fields,IEEE Transactions on Information Theory, vol. 57, no. 4, pp. 2243-2251, 2011,DOI: 10.1109/TIT.2010.2092415.

[13] B.R.Mc Donald,Finite Rings with Identity(Pure and Applied Mathematics), vol.28. Marcel Dekker ed., New York,1974,ISBN-10:0824761618.

[14] M. Miwa, T.Wadayama, and I. Takumi,A cutting-plane method based on redundant rows for improving fractional distance, IEEE Journal on SelectedAreas in Communications,vol.27,no.6,pp.1005-1012,DOI:10.1109/JSAC.2009.090818,2009.

[15] Mohammed M.Al-Ashker and Jianzhang Chen, Cyclic codes of arbitrary length over Fq+uFq+u2Fq +....+uk□1Fq ,Palestine Journal of Mathematics,vol.2,no.1,pp.72-80,2013.

[16] E.Prange,Some cyclic error-correcting codes with simple decoding algorithms." AFCRC-TN-58-156 ,1985. Simeon Ball, Cyclic Codes In:A Course in Algebraic Error-Correcting Codes,Compact Textbooks I Mathematics,Birkhauser,Cham,2020,DOI:10.1007/978-3-030-41153-4-5.

[17] J.Wolfmann,Negacyclic and cyclic codes over Z4 , IEEE Transactions onInformation Theory,vol.45,no.7,pp.2527-2532,1999,DOI:10.1109/18.796397.

[18] B.Yildiz,N.Aydin,On cyclic codes over Z4+uZ4 and Z4 images,InternationalJournal of Information coding Theory,vol.19,pp.226-237,(2014).

[19] S.Zhu, L.Wang,A class of constacyclic codes over Fp+vFp and their Gray images,Discrete Mathematics,vol.311(23-24),pp.2677-2682,(2011).